RUSH

Access DB# 160429

SEARCH REQUEST FORM

88

Scientific and Technical Information Center

Requester's Full Name: Kambiz Zand Examiner #: 78582 Date: 07/25/05
Art Unit: 2132 Phone Number ~~38~~ 23811 Serial Number: 09/632,933
Mail Box and Bldg/Room Location: 2A19 2A15 Results Format Preferred (circle): PAPER DISK E-MAIL

If more than one search is submitted, please prioritize searches in order of need.

****

Please provide a detailed statement of the search topic, and describe as specifically as possible the subject matter to be searched. Include the elected species or structures, keywords, synonyms, acronyms, and registry numbers, and combine with the concept or utility of the invention. Define any terms that may have a special meaning. Give examples or relevant citations, authors, etc, if known. Please attach a copy of the cover sheet, pertinent claims, and abstract.

Title of Invention: Synchronization of Authentication ciphering offset

Inventors (please provide full names): Persson, Joakim; Smeets, Ben; Melin, Tobias

Earliest Priority Filing Date: 08/04/2000

**For Sequence Searches Only* Please include all pertinent information (parent, child, divisional, or issued patent numbers) along with the appropriate serial number.*

Please See Attached Claims, Abstract & Specification

Thanks. I appreciate an expedite search since I am in the Second Part of the Program. Thanks

Zand

RECEIVED
JUL 26 2005
BY:

****

STAFF USE ONLY	Type of Search		Vendors and cost where applicable	
Searcher: Laurel Holloway	NA Sequence (#)		STN	
Searcher Phone #: 2-3528	AA Sequence (#)		Dialog	
Searcher Location: RND 4B19	Structure (#)		Questel/Orbit	
Date Searcher Picked Up: 7-26-05	Bibliographic	✓	Dr.Link	
Date Completed: 7-27-05	Litigation		Lexis/Nexis	
Searcher Prep & Review Time: 40	Fulltext	✓	Sequence Systems	
Clerical Prep Time:	Patent Family		WWW/Internet	✓
Online Time: 185	Other		Other (specify)	

PTO-1590 (8-01)

STIC Search Report
EIC 2100

STIC Database Tracking Number: 160429

TO:	From:
Kambiz Zand **Location: RND 2A19** **Art Unit : 2132** **Tuesday, July 26, 2005** **Case Serial Number: 09/632933**	**David Holloway** **Location: EIC 2100** **RND 4B19** **Phone: 2-3528** **david.holloway@uspto.gov**

Search Notes

Dear Examiner Zand,

Attached please find your search results for above-referenced case.
Please contact me if you have any questions or would like a re-focused search.

David

```
Set     Items   Description
S1       6562   BLUETOOTH? OR BLUE()TOOTH OR WIFI OR WAPR OR WIRELESS OR C-
            ELLULAR OR MOBILE OR 802()11 OR 802()15 OR PICONET? OR GSM OR
            UMTS OR WLAN?
S2          0   ACO OR COF OR (CYPHER? OR CIPHER?)(N)(OFFSET? OR OFF()(SETS
             OR SET))
S3       1334   SYNCRON? OR SYNCHRON? OR (RENDER? OR MAKE OR MAKING OR MAD-
            E)()(IDENTICAL? OR SAME? OR EQUIVALENT? OR EQUAL) OR IDENTICA-
            LI?
S4       1685   RESYNC? OR COOCCUR? OR CONCUR? OR MATCHING
S5       1803   AUTHENTIC? OR CHALLENGE()RESPONSE? OR CRAM OR LINK()KEY? ?
            OR KEYPAIR? OR KEY()PAIR?
S6      11955   CURRENT? OR RECENT? OR NEWEST? OR LATEST? OR LAST OR FRESH
S7       4551   SAME OR IDENTICAL OR MATCHING
S8         26   S1 AND (S3 OR S4) AND S5
S9         26   S8 NOT PY>2000
S10        11   S9 NOT PD>20000804
S11         1   S9 NOT RD>20000804
File 256:TecInfoSource 82-2005/Jun
         (c) 2005 Info.Sources Inc
```

```
Set     Items   Description
S1    3574461   BLUETOOTH? OR BLUE()TOOTH OR WIFI OR WAPR OR WIRELESS OR C-
            ELLULAR OR MOBILE OR 802()11 OR 802()15 OR PICONET? OR GSM OR
            UMTS OR WLAN?
S2      10133   ACO OR COF OR (CYPHER? OR CIPHER?)(N)(OFFSET? OR OFF()(SETS
             OR SET))
S3     403819   SYNCRON? OR SYNCHRON? OR (RENDER? OR MAKE OR MAKING OR MAD-
            E)()(IDENTICAL? OR SAME? OR EQUIVALENT? OR EQUAL) OR IDENTICA-
            LI?
S4     920946   RESYNC? OR COOCCUR? OR CONCUR? OR MATCHING
S5     489074   AUTHENTIC? OR CHALLENGE()RESPONSE? OR CRAM OR LINK()KEY? ?
            OR KEYPAIR? OR KEY()PAIR?
S6        176   S2(3N)(CURRENT? OR RECENT? OR NEWEST? OR LATEST? OR LAST OR
             FRESH)
S7         24   S2(3N)(SAME OR IDENTICAL OR MATCHING)
S8          0   S1(S)S2(4N)(S3 OR S4)
S9        168   S1(S)S2
S10         0   S2(4N)(S3 OR S4)(S)S5
S11         0   S5(S)(S6 OR S7)
S12        17   S1(5N)S2
S13         0   S9(S)S5
S14         2   S9(S)(S3 OR S4)
S15        43   S14 OR S12 OR S7
S16        28   RD (unique items)
S17        16   S16 NOT PY>2000
File 275:Gale Group Computer DB(TM) 1983-2005/Jul 26
         (c) 2005 The Gale Group
File  47:Gale Group Magazine DB(TM) 1959-2005/Jul 26
         (c) 2005 The Gale group
File  75:TGG Management Contents(R) 86-2005/Jul W3
         (c) 2005 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2005/Jul 25
         (c) 2005 The Gale Group
File  16:Gale Group PROMT(R) 1990-2005/Jul 25
         (c) 2005 The Gale Group
File 624:McGraw-Hill Publications 1985-2005/Jul 26
         (c) 2005 McGraw-Hill Co. Inc
File 484:Periodical Abs Plustext 1986-2005/Jul W3
         (c) 2005 ProQuest
File 613:PR Newswire 1999-2005/Jul 26
         (c) 2005 PR Newswire Association Inc
File 813:PR Newswire 1987-1999/Apr 30
         (c) 1999 PR Newswire Association Inc
File 141:Readers Guide 1983-2004/Dec
         (c) 2005 The HW Wilson Co
File 239:Mathsci 1940-2005/Sep
         (c) 2005 American Mathematical Society
File 370:Science 1996-1999/Jul W3
         (c) 1999 AAAS
File 696:DIALOG Telecom. Newsletters 1995-2005/Jul 26
         (c) 2005 The Dialog Corp.
File 553:Wilson Bus. Abs. FullText 1982-2004/Dec
         (c) 2005 The HW Wilson Co
File 621:Gale Group New Prod.Annou.(R) 1985-2005/Jul 26
         (c) 2005 The Gale Group
File 674:Computer News Fulltext 1989-2005/Jul W3
         (c) 2005 IDG Communications
File  88:Gale Group Business A.R.T.S. 1976-2005/Jul 25
         (c) 2005 The Gale Group
File 369:New Scientist 1994-2005/May W3
         (c) 2005 Reed Business Information Ltd.
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 635:Business Dateline(R) 1985-2005/Jul 26
```

File 15:ABI/Inform(R) 1971-2005/Jul 26

File 9:Business & Industry(R) Jul/1994-2005/Jul 25

File 13:BAMP 2005/Jul W3

File 810:Business Wire 1986-1999/Feb 28

File 610:Business Wire 1999-2005/Jul 26

File 647:CMP Computer Fulltext 1988-2005/Jul W2

File 98:General Sci Abs/Full-Text 1984-2004/Dec

File 148:Gale Group Trade & Industry DB 1976-2005/Jul 26

File 634:San Jose Mercury Jun 1985-2005/Jul 24

```
Set     Items   Description
S1    1314963   BLUETOOTH? OR BLUE()TOOTH OR WIFI OR WAPR OR WIRELESS OR C-
            ELLULAR OR MOBILE OR 802()11 OR 802()15 OR PICONET? OR GSM OR
            UMTS OR WLAN?
S2       6553   ACO OR COF OR (CYPHER? OR CIPHER?)(N)(OFFSET? OR OFF()(SETS
             OR SET))
S3     357295   SYNCRON? OR SYNCHRON? OR (RENDER? OR MAKE OR MAKING OR MAD-
            E)()(IDENTICAL? OR SAME? OR EQUIVALENT? OR EQUAL) OR IDENTICA-
            LI?
S4     525499   RESYNC? OR COOCCUR? OR CONCUR? OR MATCHING
S5      58571   AUTHENTIC? OR CHALLENGE()RESPONSE? OR CRAM OR LINK()KEY? ?
            OR KEYPAIR? OR KEY()PAIR?
S6    5776609   CURRENT? OR RECENT? OR NEWEST? OR LATEST? OR LAST OR FRESH
S7    2799533   SAME OR IDENTICAL OR MATCHING
S8          3   S1 AND S2(3N)(S3 OR S4 OR S6 OR S7)
S9          3   S1 AND S2 AND (S3 OR S4) AND S5
S10         3   S1 AND S2 AND (S6 OR S7) AND S5
S11       173   S1 AND S2
S12        55   S11 AND (S3 OR S4 OR S6 OR S7)
S13        78   S1 AND S5 AND (S3 OR S4) AND (NUMBER? OR PIN OR PSEUDORAND-
            OM? OR RANDOM? OR KEY OR KEYS OR IDENTIFIER?)
S14       133   S8 OR S9 OR S10 OR S12 OR S13
S15        93   RD (unique items)
S16        29   S15 NOT PY>2000
S17        29   S16 NOT PD=20000804:20030804
S18        29   S17 NOT PD=20030804:20050804
File   8:Ei Compendex(R) 1970-2005/Jul W3
         (c) 2005 Elsevier Eng.  Info. Inc.
File  35:Dissertation Abs Online 1861-2005/Jun
         (c) 2005 ProQuest Info&Learning
File  65:Inside Conferences 1993-2005/Jul W4
         (c) 2005 BLDSC all rts. reserv.
File   2:INSPEC 1969-2005/Jul W3
         (c) 2005 Institution of Electrical Engineers
File  94:JICST-EPlus 1985-2005/Jun W1
         (c)2005 Japan Science and Tech Corp(JST)
File 111:TGG Natl.Newspaper Index(SM) 1979-2005/Jul 25
         (c) 2005 The Gale Group
File   6:NTIS 1964-2005/Jul W3
         (c) 2005 NTIS, Intl Cpyrght All Rights Res
File 144:Pascal 1973-2005/Jul W3
         (c) 2005 INIST/CNRS
File  34:SciSearch(R) Cited Ref Sci 1990-2005/Jul W3
         (c) 2005 Inst for Sci Info
File  62:SPIN(R) 1975-2005/May W3
         (c) 2005 American Institute of Physics
File  99:Wilson Appl. Sci & Tech Abs 1983-2005/Jun
         (c) 2005 The HW Wilson Co.
File  95:TEME-Technology & Management 1989-2005/Jun W3
         (c) 2005 FIZ TECHNIK
```

18/5/1 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

05421697 E.I. No: EIP99114913470
Title: Dynamic participation in a secure conference scheme for mobile **communications**
Author: Hwang, Min-Shiang
Corporate Source: Chaoyang Univ of Technology, Wufeng, Taiwan
Source: IEEE Transactions on Vehicular Technology v 48 n 5 1999. p 1469-1474
Publication Year: 1999
CODEN: ITVTAB ISSN: 0018-9545
Language: English
Document Type: JA; (Journal Article) Treatment: T; (Theoretical)
Journal Announcement: 0001W2
Abstract: We propose a scheme to implement secure digital **mobile** communications. The scheme can both enable multiple users to hold a secure teleconference and also resolve the problem of allowing a participant to join dynamically or to quit a teleconference already in progress. Essentially, teleconference is a **synchronous** collaboration session in which participants at remote locations cooperate through **wireless** communications. Two requirements for the system are: privacy and **authentication** . Privacy signifies that an eavesdropper cannot intercept conversations of a conference. **Authentication** ensures that the service is not obtained fraudulently in order to avoid usage charge usage. We present a conference **key** distribution scheme for digital **mobile** communications, according to which users can share a common secret **key** to hold a secure teleconference over a public channel. The participants need not alter their secret information when a participant joins late or quits the conference early. (Author abstract) 24 Refs.
Descriptors: ***Cellula** r radio systems; Digital signal processing; Teleconferencing; Cryptography; **Wireless** telecommunication systems; Data privacy
Identifiers: Secure digital **mobile** communications
Classification Codes:
716.3 (Radio Systems & Equipment); 716.1 (Information & Communication Theory)
716 (Radar, Radio & TV Electronic Equipment)
71 (ELECTRONICS & COMMUNICATIONS)

18/5/2 (Item 2 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

05350285 E.I. No: EIP99094765916
Title: Proposal of secure remote access using encryption
Author: Kawase, Tetsuya; Watanabe, Akira; Sasase, Iwao
Corporate Source: Keio Univ, Yokohama, Jpn
Conference Title: Proceedings of the IEEE GLOBECOM 1998 - The Bridge to the Global Integration
Conference Location: Sydney, NSW, Aust Conference Date: 19981108-19981112
Sponsor: IEEE Communications Society; Telstra; ERICSSON; SIEMENS; et al.
E.I. Conference No.: 55358
Source: Conference Record / IEEE Global Telecommunications Conference v 2 1998. p 868-873
Publication Year: 1998
CODEN: CRIEET
Language: English
Document Type: JA; (Journal Article) Treatment: A; (Applications); T; (Theoretical)
Journal Announcement: 9910W2
Abstract: On a remote access environment, strong **authentication** of the remote user is required since the danger of stealing of **authentication** devices is very high. In this paper, we propose a secure remote access system appropriate for the remote access environment. Two **authentication** schemes are used to reduce the danger of stealing of **authentication** devices. One is the **authentication** using the public **key** cryptography. The public **key** cryptography is stored in the IC card of the remote user and the IC card is locked by the **PIN** . The another scheme is the one-time pattern **authentication** which is a sort of challenge and response. Simultaneously, simple **key** delivery is performed with these **authentication** protocol. An evaluation of our proposed scheme proves the feasibility and the efficiency as compared with the conventional system using the one-time password and Diffie-Hellman **key** agreement protocol. (Author abstract) 3 Refs.
Descriptors: ***Mobil** e computing; Security of data; Cryptography; Network protocols; Pattern **matching**
Identifiers: Secure remote access system; One-time pattern **authentication**
Classification Codes:
723.2 (Data Processing); 723.5 (Computer Applications)
716 (Radar, Radio & TV Electronic Equipment); 723 (Computer Software)
71 (ELECTRONICS & COMMUNICATIONS); 72 (COMPUTERS & DATA PROCESSING)

18/5/13 (Item 6 from file: 2)
DIALOG(R)File 2:INSPEC

6379114 INSPEC Abstract Number: B1999-11-6250F-084
Title: Dynamic participation in a secure conference scheme for mobile **communications**
Author(s): Min-Shiang Hwang
Author Affiliation: Dept. of Inf. Manage., Chaoyang Univ. of Technol., Wufeng, Taiwan
Journal: IEEE Transactions on Vehicular Technology vol.48, no.5 p. 1469-74
Publisher: IEEE,
Publication Date: Sept. 1999 Country of Publication: USA
CODEN: ITVTAB ISSN: 0018-9545
SICI: 0018-9545(199909)48:5L.1469:DPSC;1-6
Material Identity Number: I112-1999-005
U.S. Copyright Clearance Center Code: 0018-9545/99/$10.00
Document Number: S0018-9545(99)07367-3
Language: English Document Type: Journal Paper (JP)
Treatment: Theoretical (T)
Abstract: We propose a scheme to implement secure digital **mobile** communications. The scheme can both enable multiple users to hold a secure teleconference and also resolve the problem of allowing a participant to join dynamically or to quit a teleconference already in progress. Essentially, teleconference is a **synchronous** collaboration session in which participants at remote locations cooperate through **wireless** communications. Two requirements for the system are: privacy and **authentication** . Privacy signifies that an eavesdropper cannot intercept conversations of a conference. **Authentication** ensures that the service is not obtained fraudulently in order to avoid usage charge usage. We present a conference **key** distribution scheme for digital **mobile** communications, according to which users can share a common secret **key** to hold a secure teleconference over a public channel. The participants need not alter their secret information when a participant joins late or quits the conference early. (24 Refs)
Subfile: B
Descriptors: cryptography; digital radio; land **mobile** radio; message **authentication** ; telecommunication security; teleconferencing
Identifiers: dynamic participation; secure conference scheme; **mobile** communications; digital **mobile** communications; multiple users; secure teleconference; **synchronous** collaboration session; remote locations; lwireless communications; privacy; **authentication** ; eavesdropper; conversations; fraud; usage charge usage; conference **key** distribution scheme; common secret **key** ; public channel
Class Codes: B6250F (Mobile radio systems); B6210P (Teleconferencing); B6120D (Cryptography)

IEEE Xplore RELEASE 2.1

Welcome United States Patent and Trademark Office

Advanced Search

BROWSE SEARCH IEEE XPLORE GUIDE

OPTION 1
Enter keywords or phrases, select fields, and select operators

[ ] In All Fields

AND [ ] In All Fields

AND [ ] In All Fields

Run Search Reset

OPTION 2
Enter keywords, phrases, or a Boolean expression

```
(cof or aco or cipher offset or cypher
offset) and (bluetooth or wireless or
wifi or cellular or wap or wlan or
piconet or umts) <in> pdfdata
```

Run Search Reset

» Note: You may use the search operators <and> or <or> without the start and end brackets <>.

» Learn more about Field Codes, Search Examples, and Search Operators

» Publications

- Select publications
  - IEEE Periodicals
  - IEE Periodicals
  - IEEE Conference Proceedin
  - IEE Conference Proceedings
  - IEEE Standards

» Other Resources (Available for Pur

- IEEE Books

» Select date range

- Search latest content update (25
- From year 1951 to 2000

» Display Format

- Citation
- Citation & Abstra

» Organize results

Maximum 100

Display 25 results per pa

Sort by Relevance

In Descending order

Indexed by Inspec

Search Results

Results for **"(cof or aco) and (bluetooth or blue tooth) <in>pdfdata"**
Your search matched **23** of **1198558** documents.
A maximum of **100** results are displayed, **25** to a page, sorted by **Relevance** in **Descending** order.

e-mail

» Search Options

View Session History

New Search

Modify Search

(cof or aco) and (bluetooth or blue tooth) <in>pdfdata

Check to search only within this results set

Display Format: Citation Citation & Abstract

» Key

IEEE JNL	IEEE Journal or Magazine
IEE JNL	IEE Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IEE CNF	IEE Conference Proceeding
IEEE STD	IEEE Standard

Select Article Information

1. **IEEE Std 802.15.1 IEEE Standard for Information technology- Telecommu information exchange between systems- Local and metropolitan area net requirements Part 15.1: Wireless Medium Access Control (MAC) and Phy (PHY) Specifications for Wireless Personal Area Networks (WPANs)**
IEEE Std 802.15.1-2002
2002 Page(s):0_1 - 0_3
AbstractPlus | Full Text: PDF(9782 KB) **IEEE STD**

2. **Hardware implementation of Bluetooth security**
Kitsos, P.; Sklavos, N.; Papadomanolakis, K.; Koufopavlou, O.;
Pervasive Computing, IEEE
Volume 2, Issue 1, Jan-Mar 2003 Page(s):21 - 29
Digital Object Identifier 10.1109/MPRV.2003.1186722
AbstractPlus | Full Text: PDF(1744 KB) **IEEE JNL**

3. **An analysis of Bluetooth security vulnerabilities**
Hager, C.T.; Midkiff, S.F.;
Wireless Communications and Networking, 2003. WCNC 2003. 2003 IEEE
Volume 3, 16-20 March 2003 Page(s):1825 - 1831 vol.3
Digital Object Identifier 10.1109/WCNC.2003.1200664
AbstractPlus | Full Text: PDF(384 KB) **IEEE CNF**

4. **A Key Establishment Protocol for Bluetooth Scatternets**
Huaizhi Li; Singhal, M.;
Distributed Computing Systems Workshops, 2005. 25th IEEE International Co
06-10 June 2005 Page(s):610 - 616
Digital Object Identifier 10.1109/ICDCSW.2005.14
AbstractPlus | Full Text: PDF(95 KB) **IEEE CNF**

5. **A software architecture for open service gateways**
Gong, L.;
Internet Computing, IEEE
Volume 5, Issue 1, Jan.-Feb. 2001 Page(s):64 - 70
Digital Object Identifier 10.1109/4236.895144
AbstractPlus | References | Full Text: PDF(196 KB) **IEEE JNL**

6. **Microwave surfing. Wireless networks: an electronic battlefield?**

Bansal, R.;
Microwave Magazine, IEEE
Volume 2, Issue 4, Dec. 2001 Page(s):32 - 34
Digital Object Identifier 10.1109/6668.969933

AbstractPlus | References | Full Text: PDF(310 KB) **IEEE JNL**

☐ **7. Asia Pacific abstracts**
Microwave and Wireless Components Letters, IEEE [see also IEEE Microwave Wave Letters]
Volume 12, Issue 12, Dec. 2002 Page(s):513 - 578
Digital Object Identifier 10.1109/LMWC.2002.804912

AbstractPlus | Full Text: PDF(658 KB) **IEEE JNL**

☐ **8. Energy-efficient DSPs for wireless sensor networks**
Wang, A.; Chandrakasan, A.;
Signal Processing Magazine, IEEE
Volume 19, Issue 4, July 2002 Page(s):68 - 78
Digital Object Identifier 10.1109/MSP.2002.1012351

AbstractPlus | References | Full Text: PDF(2584 KB) **IEEE JNL**

☐ **9. WLAN security: current and future**
Park, J.S.; Dicoi, D.;
Internet Computing, IEEE
Volume 7, Issue 5, Sept.-Oct. 2003 Page(s):60 - 65
Digital Object Identifier 10.1109/MIC.2003.1232519

AbstractPlus | References | Full Text: PDF(376 KB) **IEEE JNL**

☐ **10. Wearable communities: augmenting social networks with wearable comp**
Kortuem, G.; Segall, Z.;
Pervasive Computing, IEEE
Volume 2, Issue 1, Jan-Mar 2003 Page(s):71 - 78
Digital Object Identifier 10.1109/MPRV.2003.1186728

AbstractPlus | Full Text: PDF(1181 KB) **IEEE JNL**

☐ **11. Using smart phones to access site-specific services**
Toye, E.; Sharp, R.; Anil Madhavapeddy; Scott, D.;
Pervasive Computing, IEEE
Volume 4, Issue 2, Jan.-March 2005 Page(s):60 - 66
Digital Object Identifier 10.1109/MPRV.2005.44

AbstractPlus | Full Text: PDF(1928 KB) **IEEE JNL**

☐ **12. Social serendipity: mobilizing social software**
Eagle, N.; Pentland, A.;
Pervasive Computing, IEEE
Volume 4, Issue 2, Jan.-March 2005 Page(s):28 - 34
Digital Object Identifier 10.1109/MPRV.2005.37

AbstractPlus | Full Text: PDF(1160 KB) **IEEE JNL**

☐ **13. 3D simultaneous localization and modeling from stereo vision**
Garcia, M.A.; Solanas, A.;
Robotics and Automation, 2004. Proceedings. ICRA '04. 2004 IEEE Internatio
Volume 1, 2004 Page(s):847 - 853 Vol.1
Digital Object Identifier 10.1109/ROBOT.2004.1307255

AbstractPlus | Full Text: PDF(693 KB) **IEEE CNF**

☐ **14. Implementation and evaluation of a low-power sound-based user activity system**
Stager, M.; Lukowicz, P.; Troster, G.;

Wearable Computers, 2004. ISWC 2004. Eighth International Symposium on
Volume 1, 31 Oct.-3 Nov. 2004 Page(s):138 - 141
Digital Object Identifier 10.1109/ISWC.2004.25
AbstractPlus | Full Text: PDF(336 KB) **IEEE CNF**

☐ **15. Table of Contents**
Circuits and Systems, 2004. ISCAS '04. Proceedings of the 2004 International
Volume 5, 23-26 May 2004 Page(s):xvii - xi
Full Text: PDF(444 KB) **IEEE CNF**

☐ **16. Table of contents**
Circuits and Systems, 2004. ISCAS '04. Proceedings of the 2004 International
Volume 1, 23-26 May 2004 Page(s):xvii - XXII
Full Text: PDF(444 KB) **IEEE CNF**

☐ **17. Table of Contents**
Circuits and Systems, 2004. ISCAS '04. Proceedings of the 2004 International
Volume 4, 23-26 May 2004 Page(s):xvii - XXII
Full Text: PDF(444 KB) **IEEE CNF**

☐ **18. Table of Contents**
Circuits and Systems, 2004. ISCAS '04. Proceedings of the 2004 International
Volume 3, 23-26 May 2004 Page(s):xvii - XXII
Full Text: PDF(444 KB) **IEEE CNF**

☐ **19. Table of contents**
Circuits and Systems, 2004. ISCAS '04. Proceedings of the 2004 International
Volume 2, 23-26 May 2004 Page(s):xvii - XXII
Full Text: PDF(444 KB) **IEEE CNF**

☐ **20. Demonstrating vulnerabilities in Bluetooth security**
Hager, C.T.; Midkiff, S.F.;
Global Telecommunications Conference, 2003. GLOBECOM '03. IEEE
Volume 3, 1-5 Dec. 2003 Page(s):1420 - 1424 vol.3
Digital Object Identifier 10.1109/GLOCOM.2003.1258472
AbstractPlus | Full Text: PDF(308 KB) **IEEE CNF**

☐ **21. 2003 IEEE International Conference On Systems, Man And Cybernetics**
Systems, Man and Cybernetics, 2003. IEEE International Conference on
Volume 3, 5-8 Oct. 2003 Page(s):i - lii
AbstractPlus | Full Text: PDF(2932 KB) **IEEE CNF**

☐ **22. 2003 IEEE International Conference on Systems, Man and Cybernetics**
Systems, Man and Cybernetics, 2003. IEEE International Conference on
Volume 1, 5-8 Oct. 2003 Page(s):i - lxiv
Digital Object Identifier 10.1109/ICSMC.2003.1243782
AbstractPlus | Full Text: PDF(3062 KB) **IEEE CNF**

☐ **23. 2003 IEEE International Conference On Systems, Man And Cybernetics**
Systems, Man and Cybernetics, 2003. IEEE International Conference on
Volume 4, 5-8 Oct. 2003 Page(s):i - lii
AbstractPlus | Full Text: PDF(2912 KB) **IEEE CNF**

View Selected Items

```
Set     Items   Description
S1     362427   BLUETOOTH? OR BLUE()TOOTH OR WIFI OR WAPR OR WIRELESS OR C-
             ELLULAR OR MOBILE OR 802()11 OR 802()15 OR PICONET? OR GSM OR
             UMTS OR WLAN?
S2       7505   ACO OR COF OR (CYPHER? OR CIPHER?)(N)(OFFSET? OR OFF()(SETS
              OR SET))
S3     121234   SYNCRON? OR SYNCHRON? OR (RENDER? OR MAKE OR MAKING OR MAD-
             E)()(IDENTICAL? OR SAME? OR EQUIVALENT? OR EQUAL) OR IDENTICA-
             LI?
S4     196877   RESYNC? OR COOCCUR? OR CONCUR? OR MATCHING
S5      40585   AUTHENTIC? OR CHALLENGE()RESPONSE? OR CRAM OR LINK()KEY? ?
             OR KEYPAIR? OR KEY()PAIR?
S6     972581   CURRENT? OR RECENT? OR NEWEST? OR LATEST? OR LAST OR FRESH
S7    1334890   SAME OR IDENTICAL OR MATCHING
S8         12   S1(3N)S2
S9          5   S2(5N)(S3 OR S4)
S10        48   S2(S)(S3 OR S4)(S)(S6 OR S7)
S11       113   S1(10N)(S4 OR S3)(10N)S5
S12        19   S11 AND IC=H04L-009
S13        10   S10 AND IC=(G06F OR H04L)
S14        44   S8 OR S9 OR S12 OR S13
S15         1   S2(2N)(S6 OR S7)(S)S5
S16        62   S2(2N)(S6 OR S7)
S17         2   S1(10N)S2(10N)(S6 OR S7 OR S3 OR S4)
S18         4   S16(S)S1
S19         1   S16(S)S5
S20         8   S16 AND IC=(G06F OR H04L)
S21        84   S8 OR S9 OR S10 OR S12 OR S13 OR S15 OR S17 OR S18 OR S19
S22        30   S21 AND IC=(G06F OR H04L)
S23        30   IDPAT (sorted in duplicate/non-duplicate order)
S24        30   IDPAT (primary/non-duplicate records only)
File 348:EUROPEAN PATENTS 1978-2005/Jul W03
         (c) 2005 European Patent Office
File 349:PCT FULLTEXT 1979-2005/UB=20050721,UT=20050714
         (c) 2005 WIPO/Univentio
```

24/3,K/2 (Item 2 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01142717
SECURE PROCESSING FOR AUTHENTICATION OF A WIRELESS COMMUNICATIONS DEVICE
SICHERE VERARBEITUNG FUR DIE AUTHENTIFIZIERUNG EINES DRAHTLOSEN KOMMUNIKATIONSGERATS
TRAITEMENT PROTEGE PERMETTANT D'AUTHENTIFIER UN DISPOSITIF DE COMMUNICATION SANS FIL
PATENT ASSIGNEE:
QUALCOMM INCORPORATED, (910897), 5775 Morehouse Drive, San Diego, CA 92121-1714, (US), (Proprietor designated states: all)
INVENTOR:
BOSTLEY, Phil, J., III, 1639 9th Street, Boulder, CO 80302, (US)
SRINIVASAN, Raghavan c/o Qualcomm Incorporated, 5775 Morehouse Drive, San Diego, CA 92121, (US)
ECKHARDT, Andrew, D. c/o Qualcomm Incorporated, 5775 Morehouse Drive, San Diego, CA 92121-1714, (US)
LEGAL REPRESENTATIVE:
Wagner, Karl H., Dipl.-Ing. (12567), Wagner & Geyer, Patentanwalte, Gewurzmuhlstrasse 5, 80538 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 1106000 A1 010613 (Basic)
EP 1106000 B1 050622
WO 2000011835 000302
APPLICATION (CC, No, Date): EP 99948053 990819; WO 99US19199 990819
PRIORITY (CC, No, Date): US 136894 980819
DESIGNATED STATES: DE; FR; GB
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: **H04L-009/32** ; H04Q-007/30
NOTE:
No A-document published by EPO
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	200525	1933
CLAIMS B	(German)	200525	1852
CLAIMS B	(French)	200525	2191
SPEC B	(English)	200525	4033
Total word count - document A			0
Total word count - document B			10009
Total word count - documents A + B			10009

INTERNATIONAL PATENT CLASS: **H04L-009/32** ...

...SPECIFICATION system and the wireless communications device share another random number. The authentication system and the **wireless** communications device each use the SSD and this other random number to generate an **authentication** result. The **wireless** communications device is **authenticated** if it transfers a **matching authentication** result to the **authentication** system. Although technically possible, it is not computationally feasible to derive the A-Key from the **authentication** result considering the vast amount of computing power and time required.
The authentication system maintains...

24/3,K/22 (Item 22 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00844636 **Image available**
METHOD AND SYSTEM FOR GENERATING A SEQUENCE NUMBER TO BE USED FOR AUTHENTICATION
PROCEDE ET SYSTEME PERMETTANT DE PRODUIRE UN NUMERO DE SEQUENCE DEVANT ETRE UTILISE A DES FINS D'AUTHENTIFICATION

Patent Applicant/Assignee:
NOKIA NETWORKS OY, Keilalahdentie 4, FIN-02150 Espoo, FI, FI (Residence), FI (Nationality), (For all designated states except: US)
Patent Applicant/Inventor:
NIEMI Valtteri, Topeliuksenkatu 32 G 11, FIN-00290 Helsinki, FI, FI (Residence), FI (Nationality), (Designated only for: US)
LAKSHMESHWAR Shreekanth, Etuniementie 4 B 13, FIN-02230 Espoo, FI, FI (Residence), IN (Nationality), (Designated only for: US)
KOVANEN Tero, Sahkoraitti 4 A 12, FIN-33720 Tampere, FI, FI (Residence), FI (Nationality), (Designated only for: US)
Legal Representative:
GRILL Matthias (et al) (agent), Tiedtke-Bahling-Kinne et al., Bavariaring 4, D-80336 Munich, DE,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200178306 A1 20011018 (WO 0178306)
Application: WO 2000EP3093 20000406 (PCT/WO EP0003093)
Priority Application: WO 2000EP3093 20000406
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 5276

Main International Patent Class: **H04L-009/12**
Fulltext Availability:
Detailed Description

Detailed Description
... static, and updates are only performed when new subscribers are entered to the database. In **UMTS** (Universal **Mobile** Telecommunications System), the sequence numbers used for **authentication** should be individual ones because of re **synchronisation** , and should therefore be stored after every **authentication** vector generation. This writing causes a high database load and may also decrease the reliability...agreement.

5
The iiivention is applicable to any system in which a sequence number-based **authentication** scheme is used, and a possibility for re- **synchrondsation** may be provided, and may for instance be used in an **UMTS** system..

The invention reduces the amount of writing operations of the database storing the information...user authentication request) and AUTS which contains
the (eventually concealed) sequence number SQNusjm of the **mobile** station MS1.

When the **authentication** centre of the home network receives such an **authentication** data request with " **synchronisation** failure indication", it acts as follows.
1) the **authentication** centre of the home network HE 4 retrieves SQNusjm by computing f5K(MACS), if concealed...

24/3,K/26 (Item 26 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00771565 **Image available**
METHOD AND APPARATUS FOR SECURELY TRANSMITTING DISTRIBUTED RAND SIGNALS FOR USE IN MOBILE STATION AUTHENTICATION
PROCEDE ET APPAREIL DESTINES A EMETTRE DE MANIERE SURE DES SIGNAUX DISTRIBUES DE VALEUR DE DEFI A USAGE D'AUTHENTIFICATION DE STATION MOBILE

Patent Applicant/Assignee:
QUALCOMM INCORPORATED, 5775 Morehouse Drive, San Diego, CA 92121-1714, US , US (Residence), US (Nationality)
Inventor(s):
ROSE Gregory G, 6 Kingston Avenue, Mortlake, NSW 2137, AU
Legal Representative:
WADSWORTH Philip R, Qualcomm Incorporated, 5775 Morehouse Drive, San Diego, CA 92121-1714, US

Patent and Priority Information (Country, Number, Date):
Patent: WO 200105091 A1 20010118 (WO 0105091)
Application: WO 2000US18687 20000707 (PCT/WO US0018687)
Priority Application: US 99350213 19990709
Designated States:
(Protection type is "patent" unless otherwise stated - for applications prior to 2004)
AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Publication Language: English
Filing Language: English
Fulltext Word Count: 7274

Main International Patent Class: **H04L-009/32**

English Abstract
A method and apparatus for generating and communicating random challenge values to **mobile** stations is disclosed that does not lose the unpredictability of a truly random number but can be simply and economically **synchronized** across **cellular** systems. The method and apparatus updates a binary number that will be used in **cellular** telephone system **authentication** procedures by applying a first algorithm to a plurality of most significant bits of a...

```
Set     Items   Description
S1     382590   BLUETOOTH? OR BLUE()TOOTH OR WIFI OR WAPR OR WIRELESS OR C-
            ELLULAR OR MOBILE OR 802()11 OR 802()15 OR PICONET? OR GSM OR
            UMTS OR WLAN?
S2       1845   ACO OR COF OR (CYPHER? OR CIPHER?)(N)(OFFSET? OR OFF()(SETS
             OR SET))
S3     338619   SYNCRON? OR SYNCHRON? OR (RENDER? OR MAKE OR MAKING OR MAD-
            E)()(IDENTICAL? OR SAME? OR EQUIVALENT? OR EQUAL) OR IDENTICA-
            LI?
S4     165082   RESYNC? OR COOCCUR? OR CONCUR? OR MATCHING
S5      36399   AUTHENTIC? OR CHALLENGE()RESPONSE? OR CRAM OR LINK()KEY? ?
            OR KEYPAIR? OR KEY()PAIR?
S6    1180466   CURRENT? OR RECENT? OR NEWEST? OR LATEST? OR LAST OR FRESH
S7    1704584   SAME OR IDENTICAL OR MATCHING
S8         60   S1 AND S2
S9          1   S8 AND (S3 OR S4)
S10       158   S1 AND S5 AND (S3 OR S4)
S11       231   S2 AND (S3 OR S4 OR S6 OR S7)
S12         7   S11 AND S1
S13        15   S2(5N)(S3 OR S4 OR S6 OR S7)
S14        44   (S10 OR S11) AND IC=H04L-009
S15        42   (S10 OR S11) AND MC=(W01-A04X OR W01-A05B OR W01-A07H2)
S16        24   S14 AND S15
S17         2   S8 AND IC=(H04L-009/12 OR H04L-009/32 OR H04L-009/08)
S18         2   S8 AND IC=H04L-009
S19         2   S8 AND MC=(W01-A04X OR W01-A05B OR W01-A07H2)
S20        43   S9 OR S12 OR S13 OR S16 OR S17 OR S18 OR S19
S21        43   IDPAT (sorted in duplicate/non-duplicate order)
S22        43   IDPAT (primary/non-duplicate records only)
S23         1   S2 AND (S3 OR S4) AND S5
S24         8   S2 AND (S3 OR S4) AND (S6 OR S7)
S25         3   S2 AND IC=H04L-009
S26         2   S2 AND MC=(W01-A04X OR W01-A05B OR W01-A07H2)
S27        11   S23:S26
S28         9   S27 NOT S20
S29         9   IDPAT (sorted in duplicate/non-duplicate order)
S30         9   IDPAT (primary/non-duplicate records only)
File 347:JAPIO Nov 1976-2005/Feb(Updated 050606)
        (c) 2005 JPO & JAPIO
File 350:Derwent WPIX 1963-2005/UD,UM &UP=200547
        (c) 2005  Thomson Derwent
```

```
Set     Items   Description
S1     382590   BLUETOOTH? OR BLUE()TOOTH OR WIFI OR WAPR OR WIRELESS OR C-
            ELLULAR OR MOBILE OR 802()11 OR 802()15 OR PICONET? OR GSM OR
            UMTS OR WLAN?
S2       1845   ACO OR COF OR (CYPHER? OR CIPHER?)(N)(OFFSET? OR OFF()(SETS
             OR SET))
S3     338619   SYNCRON? OR SYNCHRON? OR (RENDER? OR MAKE OR MAKING OR MAD-
            E)()(IDENTICAL? OR SAME? OR EQUIVALENT? OR EQUAL) OR IDENTICA-
            LI?
S4     165082   RESYNC? OR COOCCUR? OR CONCUR? OR MATCHING
S5      36399   AUTHENTIC? OR CHALLENGE()RESPONSE? OR CRAM OR LINK()KEY? ?
            OR KEYPAIR? OR KEY()PAIR?
S6    1180466   CURRENT? OR RECENT? OR NEWEST? OR LATEST? OR LAST OR FRESH
S7    1704584   SAME OR IDENTICAL OR MATCHING
S8         60   S1 AND S2
S9          1   S8 AND (S3 OR S4)
S10       158   S1 AND S5 AND (S3 OR S4)
S11       231   S2 AND (S3 OR S4 OR S6 OR S7)
S12         7   S11 AND S1
S13        15   S2(5N)(S3 OR S4 OR S6 OR S7)
S14        44   (S10 OR S11) AND IC=H04L-009
S15        42   (S10 OR S11) AND MC=(W01-A04X OR W01-A05B OR W01-A07H2)
S16        24   S14 AND S15
S17         2   S8 AND IC=(H04L-009/12 OR H04L-009/32 OR H04L-009/08)
S18         2   S8 AND IC=H04L-009
S19         2   S8 AND MC=(W01-A04X OR W01-A05B OR W01-A07H2)
S20        43   S9 OR S12 OR S13 OR S16 OR S17 OR S18 OR S19
S21        43   IDPAT (sorted in duplicate/non-duplicate order)
S22        43   IDPAT (primary/non-duplicate records only)
File 347:JAPIO Nov 1976-2005/Feb(Updated 050606)
         (c) 2005 JPO & JAPIO
File 350:Derwent WPIX 1963-2005/UD,UM &UP=200547
         (c) 2005  Thomson Derwent
```

22/5/10 (Item 10 from file: 350)
DIALOG(R)File 350:Derwent WPIX

016530053 **Image available**
WPI Acc No: 2004-688619/200467
Related WPI Acc No: 2004-688616; 2004-697572; 2004-698028
XRPX Acc No: N04-545506
Authentication **providing method for use in** wireless **communication network e.g. LAN, involves** synchronously **regenerating** authentication **key at two network nodes based upon node identifier information**
Patent Assignee: NEW MEXICO TECH RES FOUND (NEWM-N)
Inventor: SOLIMAN H
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 20040179690	A1	20040916	US 2003387711	A	20030313	200467 B
			US 2003448989	A	20030530	

Priority Applications (No Type Date): US 2003448989 A 20030530; US 2003387711 A 20030313
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20040179690	A1		36	H04L-009/00	CIP of application US 2003387711

Abstract (Basic): US 20040179690 A1

NOVELTY - The method involves providing a node identifier provided with an address and an initial **authentication** key, and installing the node identifier at one network node. The node identifier is stored at another network node, and the node identifier information is sent from one network node to the other network node. An **authentication** key is **synchronously** regenerated at two network nodes based upon node identifier information.

DETAILED DESCRIPTION - An INDEPENDENT CLAIM is also included for a network of providing secure **authentication** between **wireless** communication network nodes.

USE - Used for providing **authentication** between **wireless** communication network nodes, for exchanging digital data in a **wireless** communication network e.g. local area network (LAN).

ADVANTAGE - The method facilitates **synchronously** regenerating the **authentication** key at two network nodes based upon the node identifier information, thereby providing dynamic secure **authentication** among **wireless** communication network nodes. The method allows minimization of wasted bandwidth in **wireless** communication networks.

DESCRIPTION OF DRAWING(S) - DESCRIPTION OF DRAWING - The drawing shows an overview of a central authority (CA) generating daemons to manage users` dynamic **authentication** keys.

pp; 36 DwgNo 1a/19

Title Terms: **AUTHENTICITY** ; METHOD; **WIRELESS** ; COMMUNICATE; NETWORK; LAN; **SYNCHRONOUS** ; REGENERATE; **AUTHENTICITY** ; KEY; TWO; NETWORK; NODE; BASED ; NODE; IDENTIFY; INFORMATION
Derwent Class: T01; W01
International Patent Class (Main): **H04L-009/00**
File Segment: EPI

22/5/23 (Item 23 from file: 350)
DIALOG(R)File 350:Derwent WPIX

014511866 **Image available**
WPI Acc No: 2002-332569/200237
XRPX Acc No: N02-261218
Communication authentication **method in radio telecommunication system, involves confirming** authentication **when determined transmitted sequence number is within predetermined limit**
Patent Assignee: VODAFONE LTD (VODA-N)
Inventor: HOWARD P T
Number of Countries: 001 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
GB 2365687	A	20020220	GB 200019067	A	20000803	200237	B
GB 2365687	B	20040609	GB 200019067	A	20000803	200438	

Priority Applications (No Type Date): GB 200018950 A 20000802
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
GB 2365687	A		23	H04Q-007/38	
GB 2365687	B			H04Q-007/38	

Abstract (Basic): GB 2365687 A
NOVELTY - A sequence of numbers is generated and transmitted between a **UMTS** network and an user services identity module (USIM). Each of the transmitted number is checked before acceptance. **Authentication** is completed, when the determined sequence number is within a predetermined limit.
DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:
(a) Telecommunication system;
(b) Telecommunication network;
(c) User device for telecommunication method
USE - For **authenticating** communication in radio and **cellular** telecommunication networks (claimed).
ADVANTAGE - The process of checking the value of the sequentially generated numbers, helps to protect against unauthorized network. Subsequent failure of **synchronization** because of failure of freshness check is eliminated.
DESCRIPTION OF DRAWING(S) - The figure shows a flowchart of **authentication** process.
pp; 23 DwgNo 2/2
Title Terms: COMMUNICATE; **AUTHENTICITY** ; METHOD; RADIO; TELECOMMUNICATION; SYSTEM; CONFIRM; **AUTHENTICITY** ; DETERMINE; TRANSMIT; SEQUENCE; NUMBER; PREDETERMINED; LIMIT
Derwent Class: W01; W02
International Patent Class (Main): H04Q-007/38
International Patent Class (Additional): **H04L-009/32**
File Segment: EPI

22/5/27 (Item 27 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013797011 **Image available**
WPI Acc No: 2001-281223/200129
XRPX Acc No: N01-200535

Binary authentication **number updating method in** cellular **telephone system, involves applying block cipher to concatenated binary numbers obtained from original binary numbers to obtain updated binary number**

Patent Assignee: QUALCOMM INC (QUAL-N); ROSE G G (ROSE-I)
Inventor: ROSE G G
Number of Countries: 095 Number of Patents: 009
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200105091	A1	20010118	WO 2000US18687	A	20000707	200129	B
AU 200059238	A	20010130	AU 200059238	A	20000707	200129	
EP 1197035	A1	20020417	EP 2000945266	A	20000707	200233	
			WO 2000US18687	A	20000707		
KR 2002026529	A	20020410	KR 2002700259	A	20020108	200267	
CN 1360773	A	20020724	CN 2000810156	A	20000707	200269	
JP 2003504959	W	20030204	WO 2000US18687	A	20000707	200320	
			JP 2001510185	A	20000707		
US 6529487	B1	20030304	US 99350213	A	19990709	200320	
US 20030142644	A1	20030731	US 99350213	A	19990709	200354	
			US 2002306242	A	20021126		
BR 200012231	A	20040803	BR 200012231	A	20000707	200454	
			WO 2000US18687	A	20000707		

Priority Applications (No Type Date): US 99350213 A 19990709; US 2002306242 A 20021126
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200105091	A1	E	29	H04L-009/32	
Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW					
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TZ UG ZW					
AU 200059238	A			H04L-009/32	Based on patent WO 200105091
EP 1197035	A1	E		H04L-009/32	Based on patent WO 200105091
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI					
KR 2002026529	A			H04L-009/32	
CN 1360773	A			H04L-009/32	
JP 2003504959	W		33	H04L-009/32	Based on patent WO 200105091
US 6529487	B1			H04K-001/00	
US 20030142644	A1			H04Q-007/00	Cont of application US 99350213 Cont of patent US 6529487
BR 200012231	A			H04L-009/32	Based on patent WO 200105091

Abstract (Basic): WO 200105091 A1

NOVELTY - Maximal length shift register algorithm or pseudo random noise generation algorithm is applied to the 8 most significant bits of the original binary number and the least significant bits. The resultant bits are concatenated. A SKIPJACK block cipher is applied to the concatenated binary numbers to obtain the updated binary number.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

(a) **Cellular** base station;

(b) **Cellular** system

USE - For **authentication** of **mobile** stations by base stations in the **cellular** telephone system such as advanced **mobile** phone service (AMPS) system, IS-54, **GSM** system, IS-95 system.

ADVANTAGE - The block cipher encryption function and linear feedback shift register function ensure transmission of random challenge value to the **mobile** station without loosing unpredictability of the true random number and can be simply and economically **synchronized** across the **cellular** system.

DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of two Galois shift registers used for updating binary number.

pp; 29 DwgNo 3/5

Title Terms: BINARY; **AUTHENTICITY** ; NUMBER; UPDATE; METHOD; **CELLULAR** ; TELEPHONE; SYSTEM; APPLY; BLOCK; CIPHER; CONCATENATED; BINARY; NUMBER; OBTAIN; ORIGINAL; BINARY; NUMBER; OBTAIN; UPDATE; BINARY; NUMBER

Derwent Class: W01; W02

International Patent Class (Main): H04K-001/00; **H04L-009/32** ; H04Q-007/00

International Patent Class (Additional): G06F-015/00; **H04L-009/06** ; H04Q-007/38

File Segment: EPI

22/5/28 (Item 28 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013662808 **Image available**
WPI Acc No: 2001-147020/200115
XRPX Acc No: N01-107677

Communications systems method and arrangements for secure linking of entity authentication and ciphering key generation conducts entity authentication process using cryptography key when a cuphering offset value is generated

Patent Assignee: TELEFONAKTIEBOLAGET ERICSSON L M (TELF)
Inventor: SMEETS B J M; SMEETS B
Number of Countries: 095 Number of Patents: 007
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200101630	A1	20010104	WO 2000EP5742	A	20000621	200115	B
AU 200058176	A	20010131	AU 200058176	A	20000621	200124	
BR 200011870	A	20020305	BR 200011870	A	20000621	200225	
			WO 2000EP5742	A	20000621		
EP 1190526	A1	20020327	EP 2000943854	A	20000621	200229	
			WO 2000EP5742	A	20000621		
CN 1371565	A	20020925	CN 2000812025	A	20000621	200305	
JP 2003503896	W	20030128	WO 2000EP5742	A	20000621	200309	
			JP 2001506186	A	20000621		
US 6633979	B1	20031014	US 99344387	A	19990625	200368	

Priority Applications (No Type Date): US 99344387 A 19990625
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200101630	A1	E	22	H04L-009/32	
Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW					
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TZ UG ZW					
AU 200058176	A				Based on patent WO 200101630
BR 200011870	A			H04L-009/32	Based on patent WO 200101630
EP 1190526	A1	E		H04L-009/32	Based on patent WO 200101630
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI					
CN 1371565	A			H04L-009/32	
JP 2003503896	W		28	H04L-009/08	Based on patent WO 200101630
US 6633979	B1			G06F-001/24	

Abstract (Basic): WO 200101630 A1

NOVELTY - The method uses an authentication pprocess to generate a **ciphering offset** value (50). Each node (12,14) stores offset value and uses it to generate subsequent ciphering keys employed to encrypt data transmitted between the nodes, so a logical relationship between the **latest** entity authentication process and subsequently generated ciphering keys increasing the security and reduce overheads.

DETAILED DESCRIPTION - Independent claims describe an arrangement for generating ciphering keys in a communication node and a system.

USE - As a method and arrangements for secure linking of entity authentication and ciphering key generation.

ADVANTAGE - Can enhance security in any communication system including a **mobile** telecommunications system, for example, a global system for **mobile** (**GSM**) communications syatem.

DESCRIPTION OF DRAWING(S) - The drawing shows a block diagram depicting an improved authentication process and arrangement associated with secure communications system, for example.

the **ciphering offset** value (50)

the nodes (12 and 14)

pp; 22 DwgNo 4/7
Title Terms: COMMUNICATE; SYSTEM; METHOD; ARRANGE; SECURE; LINK; ENTITY; AUTHENTICITY; CIPHER; KEY; GENERATE; CONDUCTING; ENTITY; AUTHENTICITY; PROCESS; KEY; OFFSET; VALUE; GENERATE
Derwent Class: W01; W02
International Patent Class (Main): G06F-001/24; **H04L-009/08** ; **H04L-009/32**

International Patent Class (Additional): H04Q-007/38
File Segment: EPI

22/5/32 (Item 32 from file: 350)
DIALOG(R)File 350:Derwent WPIX

010742798 **Image available**
WPI Acc No: 1996-239753/199624
XRPX Acc No: N96-200648
Secure identification method for mobile **user in communication with distributed users - encrypting user's identity and/or his password and** synchronisation **indication under secret one-way function and sending encrypted message to user's home authority where he is registered**
Patent Assignee: INT BUSINESS MACHINES CORP (IBMC); IBM CORP (IBMC)
Inventor: TSUDIK G
Number of Countries: 027 Number of Patents: 015
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
WO 9613920	A1	19960509	WO 94EP3542	A	19941027	199624 B
EP 788688	A1	19970813	WO 94EP3542	A	19941027	199737
			EP 95900091	A	19941027	
JP 9511888	W	19971125	WO 94EP3542	A	19941027	199806
			JP 96514266	A	19941027	
HU 77782	T	19980828	WO 94EP3542	A	19941027	199844
			HU 981058	A	19941027	
KR 97706669	A	19971103	WO 94EP3542	A	19941027	199844
			KR 97701860	A	19970321	
US 6072875	A	20000606	WO 94EP3542	A	19941027	200033
			US 97845796	A	19970425	
RU 2150790	C1	20000610	WO 94EP3542	A	19941027	200058
			RU 97108167	A	19941027	
KR 211426	B1	19990802	WO 94EP3542	A	19941027	200104
			KR 97701860	A	19970321	
CZ 289189	B6	20011114	WO 94EP3542	A	19941027	200175
			CZ 97881	A	19941027	
CZ 9700881	A3	20011114	WO 94EP3542	A	19941027	200175
			CZ 97881	A	19941027	
CN 1164307	A	19971105	CN 94195191	A	19941027	200320
			WO 94EP3542	A	19941027	
EP 788688	B1	20040121	WO 94EP3542	A	19941027	200410
			EP 95900091	A	19941027	
DE 69433509	E	20040226	DE 94633509	A	19941027	200419
			WO 94EP3542	A	19941027	
			EP 95900091	A	19941027	
CA 2203131	C	20040330	CA 2203131	A	19941027	200424
			WO 94EP3542	A	19941027	
JP 3566298	B2	20040915	WO 94EP3542	A	19941027	200460
			JP 96514266	A	19941027	

Priority Applications (No Type Date): WO 94EP3542 A 19941027
Cited Patents: 4.Jnl.Ref; EP 532227
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9613920	A1	E	32	H04L-009/32	
Designated States (National): BR CA CN CZ HU JP KR PL RU US					
Designated States (Regional): AT BE CH DE DK ES FR GB GR IE IT LU MC NL PT SE					
EP 788688	A1	E			Based on patent WO 9613920
Designated States (Regional): AT BE CH DE ES FR GB IT LI NL SE					
JP 9511888	W		39	H04L-009/32	Based on patent WO 9613920
HU 77782	T				Based on patent WO 9613920
KR 97706669	A				Based on patent WO 9613920
US 6072875	A			H04M-001/66	Cont of application WO 94EP3542
RU 2150790	C1			H04L-009/32	Based on patent WO 9613920
KR 211426	B1			H04L-009/32	
CZ 289189	B6			H04L-009/32	Previous Publ. patent CZ 9700881
					Based on patent WO 9613920
CZ 9700881	A3			H04L-009/32	Based on patent WO 9613920

CN 1164307	A		H04L-009/32	Based on patent WO 9613920
EP 788688	B1 E		H04L-009/32	Based on patent WO 9613920
Designated States (Regional): AT BE CH DE ES FR GB IT LI NL SE				
DE 69433509	E		H04L-009/32	Based on patent EP 788688
				Based on patent WO 9613920
CA 2203131	C E		H04L-009/32	Based on patent WO 9613920
JP 3566298	B2	16	H04L-009/32	Previous Publ. patent JP 9511888
				Based on patent WO 9613920

Abstract (Basic): WO 9613920 A

The method for secure identification of a **mobile** user involves a **synchronisation** indication, pref. applying a time interval indication **synchronising** the user's input in a foreign domain with his home domain. At least one of the group consisting of an identifer, the time interval or other **synchronisation** indication and the users password or other secret **authenticator** are encrypted under a secret function, particularly a one-way function, and an encrypted message is built. The user's home domain is then indicated to the foreign domain from which the user intends to communicate.

The encrypted message is transmitted to the user's home domain. The encrypted message is evaluated in the user's home domain to determine the true identity of the user.

ADVANTAGE - Minimizes or avoids traceability and identification of **mobile** user by assigning temporary, simple, one-time aliases to travelling users. Method is efficient and not specific to particular hardware.

Dwg.3/5

Title Terms: SECURE; IDENTIFY; METHOD; **MOBILE** ; USER; COMMUNICATE; DISTRIBUTE; USER; USER; IDENTIFY; PASSWORD; **SYNCHRONISATION** ; INDICATE; SECRET; ONE; WAY; FUNCTION; SEND; ENCRYPTION; MESSAGE; USER; HOME; AUTHORISE; REGISTER

Derwent Class: P85; W01

International Patent Class (Main): **H04L-009/32** ; H04M-001/66

International Patent Class (Additional): G06F-012/14; G06F-015/00; G06K-019/07; G09C-001/00; H04Q-007/38

File Segment: EPI; EngPI

22/5/33 (Item 33 from file: 350)
DIALOG(R)File 350:Derwent WPIX

009594417
WPI Acc No: 1993-287963/199336
XRPX Acc No: N93-221527
Rolling key re- synchronisation **for** cellular **verification and validation system - setting network rolling key input to selected value and commanding** mobile **station to set it's rolling key input to same value**
Patent Assignee: ERICSSON GE MOBILE COMMUNICATIONS (TELF)
Inventor: RAITH K A
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
US 5241598	A	19930831	US 91704133	A	19910522	199336	B

Priority Applications (No Type Date): US 91704133 A 19910522
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 5241598	A		34	H04L-009/08	

Abstract (Basic): US 5241598 A
A method for the re- **synchronisation** of a rolling key in a radio network providing service to a **mobile** station. The rolling key is used as an input value among a number of input values to an **authentication** processor in each of the network and the **mobile** station. The method involves setting the network rolling key input value to a selected value. The **mobile** station commanded to set it's rolling key input value to the selected value. The selected value is a value known to the network and the **mobile** station and is selected from a group consisting of a fixed or a variable value or a combination the two.
USE/ADVANTAGE - **Authentication** of connection at hands-free or initial channel designation. Reduced **cellular** fraud.
Dwg.1/10
Title Terms: ROLL; KEY; **SYNCHRONISATION** ; **CELLULAR** ; VERIFICATION; VALID; SYSTEM; SET; NETWORK; ROLL; KEY; INPUT; SELECT; VALUE; COMMAND; **MOBILE** ; STATION; SET; ROLL; KEY; INPUT; VALUE
Index Terms/Additional Words: **ROLL_KEY_SYNCHR ONRollin g key** ; KEY; **SYNCHRON**
Derwent Class: W01; W02
International Patent Class (Main): **H04L-009/08**
International Patent Class (Additional): **H04L-009/32**
File Segment: EPI

```
Set     Items   Description
S1       1069   AU=(PERSSON J? OR PERSSON, J?)
S2        147   AU=(SMEETS B? OR SMEETS, B?)
S3        290   AU=(MELIN T? OR MELIN, T?)
S4          0   S1 AND S2 AND S3
S5         62   S1:S3 AND (CYPHER? OR CIPHER? OR ENCIPHER? OR ENCYPHER? OR
               ENCRYPT? OR CRYPTOG? OR ACO OR AUTHENTICAT?)
S6          0   S5 AND (SYNC OR SYNCS OR SYNCHRON? OR SYNCRON? OR MATCHING
               OR ASYNC?)
S7          0   S5 AND ACO
S8          0   S1:S3 AND ACO
S9         40   S5 AND AUTHENTICAT?
S10        16   RD (unique items)
S11        25   RD S5 (unique items)
S12        24   S11 NOT PY>2000
File   2:INSPEC 1969-2005/Jul W3
         (c) 2005 Institution of Electrical Engineers
File   6:NTIS 1964-2005/Jul W3
         (c) 2005 NTIS, Intl Cpyrght All Rights Res
File   8:Ei Compendex(R) 1970-2005/Jul W3
         (c) 2005 Elsevier Eng.  Info. Inc.
File  34:SciSearch(R) Cited Ref Sci 1990-2005/Jul W3
         (c) 2005 Inst for Sci Info
File  64:Environmental Engineering Abstracts 2005/May
         (c) 2005 CSA.
File  65:Inside Conferences 1993-2005/Jul W4
         (c) 2005 BLDSC all rts. reserv.
File  94:JICST-EPlus 1985-2005/Jun W1
         (c)2005 Japan Science and Tech Corp(JST)
File  95:TEME-Technology & Management 1989-2005/Jun W3
         (c) 2005 FIZ TECHNIK
File  99:Wilson Appl. Sci & Tech Abs 1983-2005/Jun
         (c) 2005 The HW Wilson Co.
File 636:Gale Group Newsletter DB(TM) 1987-2005/Jul 25
         (c) 2005 The Gale Group
File 647:CMP  Computer Fulltext 1988-2005/Jul W2
         (c) 2005 CMP Media, LLC
File 674:Computer News Fulltext 1989-2005/Jul W3
         (c) 2005 IDG Communications
File 275:Gale Group Computer DB(TM) 1983-2005/Jul 26
         (c) 2005 The Gale Group
File 239:Mathsci 1940-2005/Sep
         (c) 2005 American Mathematical Society
```

12/5/3 (Item 3 from file: 2)
DIALOG(R)File 2:INSPEC

6031439 INSPEC Abstract Number: B9811-6120B-020, C9811-6130S-018
Title: Unconditionally secure group authentication
Author(s): Van Dijk, M.; Gehrmann, C.; **Smeets, B.**
Author Affiliation: Philips Res. Lab., Eindhoven, Netherlands
Journal: Designs, Codes and Cryptography vol.14, no.3 p.281-96
Publisher: Kluwer Academic Publishers,
Publication Date: Sept. 1998 Country of Publication: Netherlands
ISSN: 0925-1022
SICI: 0925-1022(199809)14:3L.281:USGA;1-D
Material Identity Number: O660-98006
U.S. Copyright Clearance Center Code: 0925-1022/98/$9.50
Language: English Document Type: Journal Paper (JP)
Treatment: Theoretical (T)
Abstract: Group **authentication** schemes as introduced by Boyd (1989) and by Desmedt and Frankel (1992) are **cryptographic** schemes in which only certain designated groups can provide messages with **authentication** information. We study unconditionally secure group **authentication** schemes based on linear perfect secret sharing and **authentication** schemes, for which we give expressions for the probabilities of successful attacks. Furthermore, we give a construction that uses maximum rank distance codes. (18 Refs)
Subfile: B C
Descriptors: **cryptography** ; data privacy; group theory; linear codes; matrix algebra; message **authentication** ; probability
Identifiers: unconditional security; group **authentication** ; **cryptographic** schemes; message **authentication** ; linear perfect secret sharing; probabilities; attacks; maximum rank distance codes
Class Codes: B6120B (Codes); B0290H (Linear algebra); B0250 (Combinatorial mathematics); C6130S (Data security); C4140 (Linear algebra) ; C1160 (Combinatorial mathematics)

12/5/7 (Item 7 from file: 2)
DIALOG(R)File 2:INSPEC

5234395 INSPEC Abstract Number: B9605-6120B-111
Title: On the cardinality of systematic authentication **codes via error-correcting codes**
Author(s): Kabatianskii, G.A.; **Smeets, B.** ; Johansson, T.
Author Affiliation: Inst. of Inf. Transmission Problems, Acad. of Sci., Moscow, Russia
Journal: IEEE Transactions on Information Theory vol.42, no.2 p. 566-78
Publisher: IEEE,
Publication Date: March 1996 Country of Publication: USA
CODEN: IETTAW ISSN: 0018-9448
SICI: 0018-9448(199603)42:2L.566:CSAC;1-L
Material Identity Number: I044-96004
U.S. Copyright Clearance Center Code: 0018-9448/96/$05.00
Document Number: S0018-9448(96)01185-6
Language: English Document Type: Journal Paper (JP)
Treatment: Practical (P); Theoretical (T)
Abstract: In both open and private communication the participants face potential threats from a malicious enemy who has access to the communication channel and can insert messages (impersonation attack) or alter already transmitted messages (substitution attack). **Authentication** codes (A-codes) have been developed to provide protection against these threats. In this paper we introduce a new distance, called the **authentication** distance (A-distance), and show that an A-code can be described as a code for the A-distance. The A-distance is directly related to the probability P/sub S/ of success in a substitution attack. We show how to transform an error-correcting code into an A-code and vice versa. We further use these transformations to provide both upper and lower bounds on the size of the information to be **authenticated** , and study their asymptotic behavior. As examples of obtained results, we prove that the cardinality of the source state space grows exponentially with the number of keys provided P/sub S/>P/sub I/, we generalize the square-root bound given by Gilbert, MacWilliams, and Sloane in 1979, and we provide very efficient constructions using concatenated Reed-Solomon codes. (24 Refs)
Subfile: B
Descriptors: concatenated codes; error correction codes; message **authentication** ; probability; public key **cryptography** ; Reed-Solomon codes
Identifiers: cardinality; systematic **authentication** codes; error-correcting codes; private communication; open communication; communication channel; impersonation attack; substitution attack; A-codes; threats; **authentication** distance; A-distance; probability; lower bounds; upper bounds; asymptotic behavior; source state space; square-root bound; concatenated Reed-Solomon codes; universal hash functions; information integrity
Class Codes: B6120B (Codes); B0240Z (Other topics in statistics)

12/5/10 (Item 10 from file: 2)
DIALOG(R)File 2:INSPEC

4820652 INSPEC Abstract Number: B9412-6120B-107, C9412-6130S-050
Title: Bounds on the probability of deception in multiple authentication
Author(s): **Smeets, B.**
Author Affiliation: Dept. of Inf. Theory, Lund Univ., Sweden
Journal: IEEE Transactions on Information Theory vol.40, no.5 p. 1586-91
Publication Date: Sept. 1994 Country of Publication: USA
CODEN: IETTAW ISSN: 0018-9448
U.S. Copyright Clearance Center Code: 0018-9448/94/$04.00
Language: English Document Type: Journal Paper (JP)
Treatment: Theoretical (T)
Abstract: The frequently assumed "freshness" constraint on the source states in multiple **authentication** schemes is not necessary if one allows the encoding rule to change between subsequent transmissions. In the paper it is shown that the main existing lower bounds on the probabilities of successful attack on multiple **authentication** schemes also hold for this new setup. Furthermore, Stinson's (1988) bound for the substitution attack is strengthened. (20 Refs)
Subfile: B C
Descriptors: encoding; message **authentication** ; probability
Identifiers: probability of deception; multiple **authentication** ; freshness constraint; source states; encoding rule; subsequent transmissions; lower bounds; successful attack; Stinson's bound; substitution attack
Class Codes: B6120B (Codes); B0240Z (Other and miscellaneous); C6130S (Data security); C1140Z (Other and miscellaneous); C1260 (Information theory)

12/5/22 (Item 1 from file: 239)
DIALOG(R)File 239:Mathsci

02928282 MR 99h#94055
On message and key equivocation in secrecy systems.
Shtarkov, Yu. M.
Yukhanson, T.
Smits, B. Dzh. M.
(Johansson, Thomas; **Smeets, Bernard J. M.**)
Problems Inform. Transmission
Problems of Information Transmission, 1998, 34, no. 2, 197--206
ISSN: 0032-9460 CODEN: PRITA9
Source: Problemy Peredachi Informatsii, (1998),, 34, no. 2,, 117--127 ISSN: 0555-2923
Language: English
Original Language: Russian Original Summary Language: Russian
Document Type: Journal; Journal Translation
Journal Announcement: 9905
Subfile: MR (Mathematical Reviews) AMS
Abstract Length: SHORT (5 lines)
Summary (translated from the Russian): ``We study two methods (including randomization) for increasing the uncertainty concerning $n\geq 1$ transmitted messages and the key used. In addition, we show that the methods, which are equally effective for $n=1$, may perform differently for $n>1$.''
Reviewer: Summary
Reviewed from: Reviewed from original
Review Type: Abstract
Descriptors: *94A60 -Information and communication, circuits-
Communication, information- **Cryptography** (See also 11T71, 68P25)

```
Set     Items   Description
S1        270   AU=(PERSSON J? OR PERSSON, J?)
S2        112   AU=(SMEETS B? OR SMEETS, B?)
S3         31   AU=(MELIN T? OR MELIN, T?)
S4          3   S1 AND S2 AND S3
S5         71   S1:S3 AND (CYPHER? OR CIPHER? OR ENCIPHER? OR ENCYPHER? OR
               ENCRYPT? OR CRYPTOG? OR ACO OR AUTHENTICAT?)
S6         39   S5 AND IC=H04L-009
S7          3   S6 AND (SYNC OR SYNCS OR SYNCHRON? OR SYNCRON? OR MATCHING
               OR ASYNC?)
S8          2   S6 AND ACO
S9          3   S4 OR S7 OR S8
File 344:Chinese Patents Abs Aug 1985-2005/May
         (c) 2005 European Patent Office
File 347:JAPIO Nov 1976-2005/Feb(Updated 050606)
         (c) 2005 JPO & JAPIO
File 348:EUROPEAN PATENTS 1978-2005/Jul W03
         (c) 2005 European Patent Office
File 349:PCT FULLTEXT 1979-2005/UB=20050721,UT=20050714
         (c) 2005 WIPO/Univentio
File 350:Derwent WPIX 1963-2005/UD,UM &UP=200547
         (c) 2005  Thomson Derwent
```

9/5/3 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX

013924132 **Image available**
WPI Acc No: 2001-408345/200143
XRPX Acc No: N01-302165
Synchronization **of** authentication ciphering **offset e.g. for Bluetooth applications to avoid devices generating out of** synchronization **values**
Patent Assignee: TELEFONAKTIEBOLAGET ERICSSON L M (TELF)
Inventor: **MELIN T** ; **PERSSON J** ; **SMEETS B**
Number of Countries: 094 Number of Patents: 005
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 200141358	A2	20010607	WO 2000EP11780	A	20001127	200143	B
AU 200123595	A	20010612	AU 200123595	A	20001127	200154	
EP 1234405	A2	20020828	EP 2000987297	A	20001127	200264	
			WO 2000EP11780	A	20001127		
JP 2003516097	W	20030507	WO 2000EP11780	A	20001127	200331	
			JP 2001542507	A	20001127		
CN 1433610	A	20030730	CN 2000818756	A	20001127	200365	

Priority Applications (No Type Date): US 2000632933 A 20000804; US 99168375 P 19991202
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 200141358	A2	E	30	H04L-009/32	
Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG UZ VN YU ZA ZW					
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZW					
AU 200123595	A			H04L-009/32	Based on patent WO 200141358
EP 1234405	A2	E		H04L-009/32	Based on patent WO 200141358
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI TR					
JP 2003516097	W		38	H04L-009/08	Based on patent WO 200141358
CN 1433610	A			H04L-009/32	

Abstract (Basic): WO 200141358 A2
NOVELTY - An **authentication ciphering** offset (**ACO**) is generated as a function of several parameters. Several of the parameters is derived from earlier-computed values of the **ACO** .
USE - For communication system e.g. Bluetooth type application where device s experience non-controllable delays in an interface between an real-time layer and a non real-time layer.
ADVANTAGE - Enables each device to avoid generating an **ACO** value that is out of **synchronization** with a counterpart **ACO** value generated in another communication device.
DESCRIPTION OF DRAWING(S) - The drawing shows a block diagram of two devices communicating using e.g. Bluetooth.
pp; 30 DwgNo 1/7
Title Terms: **SYNCHRONISATION** ; AUTHENTICITY; **CIPHER** ; OFFSET; APPLY; AVOID; DEVICE; GENERATE; **SYNCHRONISATION** ; VALUE
Derwent Class: W01
International Patent Class (Main): **H04L-009/08** ; **H04L-009/32**
International Patent Class (Additional): **H04L-009/12**
File Segment: EPI

Your SELECT statement is:
s (bluetooth or blue()tooth)(5n)(afo or cof or cypher()offset)(5n)(sync or synchron? or syncroni? or syncs)

Items	File
Examined 50	files
Examined 100	files
Examined 150	files
Examined 200	files
Examined 250	files
Examined 300	files
Examined 350	files
Examined 400	files
Examined 450	files
Examined 500	files
Examined 550	files

No files have one or more items; file list includes 571 files.
One or more terms were invalid in 3 files.

```
Set     Items   Description
S1          3   (BLUETOOTH OR BLUE()TOOTH) AND (AFO OR COF OR (CIPHER? OR -
              CYPHER?)(N)(OFF()SET OR OFFSET))(5N)(SYNC OR SYNCHRON? OR SYN-
              CRONI? OR SYNCS)
File 342:Derwent Patents Citation Indx 1978-05/200545
         (c) 2005 Thomson Derwent
File 349:PCT FULLTEXT 1979-2005/UB=20050721,UT=20050714
         (c) 2005 WIPO/Univentio
File 351:Derwent WPI 1963-2005/UD,UM &UP=200547
         (c) 2005  Thomson Derwent
```